Source Code Analysis Tools - References

Cigital, Inc.

2006-06-12

Content area bibliography.

Aleph One. “Smashing the Stack for Fun and Profit.” *Phrack Magazine 7*, 49 (1996): File 14 of 16. http://www.phrack.org/phrack/49/P49-14.

Anderson, Robert H. & Hearn, Anthony C. *An Exploration of Cyberspace Security R&D Investment Strategies for DARPA: The Day After... in Cyberspace II*. RAND Corporation. MR-797-DARPA, 1996.

Anderson, Ross. *Security Engineering*. New York, NY: John Wiley & Sons, 2001.

AusCERT. *A Lab Engineer’s Check List for Writing Secure Unix Code*. Australian Computer Emergency Response Team, 1996.

Bellovin, Steven M. *Shifting the Odds--Writing (More) Secure Software*. Murray Hill, NJ: AT&T Research, 1994.

Boehm, Barry W. “A Spiral Model of Software Development and Enhancement.” *Computer 21*, 5 (May 1988): 61-72.

Boehm, Barry W. “Improving Software Productivity.” *Computer 20*, 9 (September 1987): 43-57.

Boehm, Barry W. & Papaccio, Philip N. “Understanding and Controlling Software Costs. *IEEE Transactions on Software Engineering 14*, 10 (October 1988): 1462-1477.

Boehm, Barry W. *Software Engineering Economics*. Englewood Cliffs, NJ: Prentice-Hall, 1981.

Bishop, Matt. *Computer Security: Art and Science*. Boston, MA: Addison-Wesley Professional, 2002.

CERT/CC. *CERT Survivability Project Report*. CERT Coordination Center, 1996.

Chess, Brian & McGraw, Gary. “Static Analysis for Security.” *IEEE Security and Privacy 2*, 6 (December 2004): 76-79.

Clements, Paul; Bachmann, Felix; Bass, Len; Garlan, David; Ivers, James; Little, Reed; Nord, Robert; & Stafford, Judith. *Documenting Software Architectures: Views and Beyond*. Boston, MA: Addison-Wesley, 2002.

Cowan, Crispin; Wagle, Perry; Pu, Calton; Beattie, Steve; & Walpole, Jonathan. “Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade.” *Proceedings of DARPA Information Survivability Conference and Expo (DISCEX)*, 1999.

Cowan, Crispin; Beattie, Steve; Finnin Day, Ryab; Pu, Calton; Wagle, Perry; & Walthinsen, Erik. “Protecting Systems from Stack Smashing Attacks with StackGuard.” *Proceedings of the 1998 Usenix Security Conference*, 1998.

Demarco, Tom & Lister, Timothy. *Waltzing With Bears: Managing Risk on Software Projects*. New York, NY: Dorset House Publishing Company, 2003.

Du, Wenliang. “Categorization of Software Errors That Led to Security Breaches.” *Proceedings of the 21st National Information Systems Security Conference*. Crystal City, Virginia, Oct. 6-9, 1998.

http://csrc.nist.gov/nissc/1998/papers.html.

Fenton, Noramn E.. & Pfleeger, Shari Lawrence. *Software Metrics: A Rigorous and Practical Approach*, 2nd ed. New York, NY: International Thomson Computer Press, 1996.

Garfinkel, Simson; Spafford, Gene; & Schwartz, Alan. *Practical Unix & Internet Security*, 3rd ed. Sebastopol, CA: O'Reilly & Associates, Inc., 2003.

Gilb, Tom. *Principles of Software Engineering*. Workingham, England: Addison-Wesley, 1988.

Ghosh, Anup K.; O'Connor, Tom; & McGraw, Gary. "An Automated Approach for Identifying Potential Vulnerabilities in Software," 104-114. *Proceedings of the 1998 IEEE Symposium on Security and Privacy*. Oakland, California, May 3-6, 1998. Los Alamitos, CA: IEEE Computer Society Press, 1998.

Gong, Li. *Inside Java 2 Platform Security*. Reading, MA: Addison Wesley, 1999.

Graff, Mark G. & Van Wyk, Kenneth R. *Secure Coding: Principles and Practices*. Sebastopol, CA: O'Reilly, 2003.

Hoglund, Greg & McGraw, Gary. *Exploiting Software : How to Break Code*. Boston, MA: Addison-Wesley, 2004.

Howard, Michael. *Designing Secure Web-Based Applications for Microsoft Windows 2000*. Redmond, WA: Microsoft Press, 2000.

Howard, Michael & LeBlanc, David C. *Writing Secure Code*, 2nd ed. Redmond, WA: Microsoft Press, 2002.

Jones, Capers. *Applied Software Measurement: Assuring Productivity and Quality*. New York, NY: McGraw-Hill, 1991.

Jones, Capers. *Assessment and Control of Software Risks*. Englewood Cliffs, NJ: Yourdon Press, 1994.

Jones, Capers. *Programming Productivity*. New York, NY: McGraw-Hill, 1986.

Kitson, David H. & Masters, Stephen. "An Analysis of SEI Software Process Assessment Results, 1987-1991," 68-77. *Proceedings of the Fifteenth International Conference on Software Engineering*. Baltimore, Maryland. May 17-21, 1993. Washington, DC: IEEE Computer Society Press, 1993.

Kuperman, Benjamin A. & Spafford, Eugene. *Generation of Application Level Audit Data via Library Interposition*. CERIAS Tech Report TR-99-11, 1999.

Maguire, Steve. *Writing Solid Code: Microsoft's Techniques for Developing Bug-Free C Programs*. Redmond, WA: Microsoft Press, 1993.

McConnell, Steve. *Code Complete: A Practical Handbook of Software Construction*. Redmond, WA: Microsoft Press, 1993.

McGraw, Gary. "Software Security." *IEEE Security and Privacy 2*, 2 (March-April 2004): 80-83.

McGraw, Gary. "From the Ground Up: The DIMACS Software Security Workshop." *IEEE Security and Privacy 1*, 2 (March-April 2003): 59-66.

McGraw, Gary. "Managing Software Security Risks." *Computer 35*, 4 (March 2002): 99-101.

McGraw, Gary & Potter, Bruce. "Software Security Testing." *IEEE Security and Privacy 2*, 5 (September-October 2004): 81-85.

McGraw, Gary, & Felten, Edward W. *Securing Java: Getting Down to Business with Mobile Code*, 2nd ed. New York, NY: John Wiley & Sons, 1999.

Miller, Barton P. “An Empirical Study of the Reliability of UNIX Utilities.” *Communications of the ACM 33*, 12 (1990).

National Center for Supercomputing Applications. *NCSA Secure Programming Guidelines*. http://archive.ncsa.uiuc.edu/General/Grid/ACES/security/programming/ (1997).

Peikari, Cyrus & Chuvakin, Anton. *Security Warrior*. Sebastopol, CA: O’Reilly, 2004.

Saltzer, Jerome H. & Schroeder, Michael D. “The Protection of Information in Computer Systems.” *Proceedings of the IEEE 63*, 9 (September 1975): 1278-1308.

Sessions, Roger. *Software Fortresses: Modeling Enterprise Architectures*. Boston, MA: Addison-Wesley, 2003.

SSwiderski, Frank & Snyder, Window. *Threat Modeling*. Redmond, WA: Microsoft Press, 2004.

Soo Hoo, Kevin; Sudbury, Andrew W.; & Jaquith, Andrew R. “Tangible ROI through Secure Software Engineering.” *Secure Business Quarterly 1*, 2 (2001).

Spafford, Eugene H. “Crisis and Aftermath.” *Communications of the ACM 32*, 6 (1989).

Spafford, Eugene H. *UNIX and Security: The Influences of History. Information Systems Security*. Auerbach Publications, 1995.

Sun Microsystems. *Security Code Guidelines*. http://java.sun.com/security/seccodeguide.html (2000).

Swanson, Marianne & Guttman, Barbara. *Generally Accepted Principles and Practices for Securing Information Technology Systems*. National Institute of Standards and Guidelines Computer Security Special Publication 800-14, 1996.

Thompson, Ken. “Reflections on Trusting Trust.” *Communications of the ACM 27*, 8 (August 1984).

Viega, John; McGraw, Gary; Mutdoseh, Tom; & Felten, Edward W. “Statically Scanning Java Code: Finding Security Vulnerabilities.” *IEEE Software 17*, 5 (September-October 2000): 68-77.

Viega, John & McGraw, Gary. *Building Secure Software: How to Avoid Security Problems the Right Way*. Boston, MA: Addison-Wesley Professional, 2001.

Viega, John & Messier, Matt. *Secure Programming Cookbook for C and C++*. Sebastopol, CA: O'Reilly, 2003 (ISBN: 0596003943).

Voas, Jeffrey & McGraw, Gary. *Software Fault Injection: Inoculating Programs Against Errors*. New York, NY: John Wiley & Sons, 1997.

Whittaker, James A.; Thompson, Herbert H.; & Thompson, Herbert. *How to Break Software Security*. Boston, MA: Addison Wesley, 2004 (ISBN: 0321194330).

Yoder, Joseph & Barcalow, Jeffrey. “Architectural Patterns for Enabling Application Security.” *Proceedings of the 1997 Pattern Languages of Programming Conference*. Monticello, Illinois, Sept. 3-5, 1997. Washington University Technical Report (wucs-97-34). http://st-www.cs.uiuc.edu/~hanmer/PLoP-97/Proceedings/proceedings.zip (1998).

Cigital, Inc. Copyright

Fields

Name	Value
Copyright Holder	Cigital, Inc.

Fields

Name	Value
is-content-area-overview	false
Content Areas	Tools/Code Analysis
SDLC Relevance	Testing
Workflow State	Publishable

[1] mailto:copyright@cigital.com